Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of the claims in the application.

Listing of Claims

1. (currently amended) A method of biometric verification using an access software application locally stored on a device and configured to access another application, system or other software entity on said device to protect biometric data against spoofing or theft, the method comprising the steps:

(a) establishing parameters of the access software application;

(b) generating a biometric template for a user by sampling;

(c) integrating into the access software application, by means of partial evaluation, the parameters and the biometric template without otherwise storing said biometric template on said device;

(d) performing tamper-resistant software (TRS) encoding to the access software application including storing the biometric ~~data~~ template in an encoded format that is irreversible, the step of performing TRS encoding being performed according to one of the following:

(i) prior to the establishing of parameters, whereby one TRS implementation covers multiple platforms and multiple biometric templates;

(ii) after the establishing of parameters and before generating the biometric template, whereby one TRS implementation covers one platform only and multiple biometric templates; and

(iii) after the establishing of parameters and after generating the biometric template, whereby one TRS implementation covers one platform only and one biometric template only;

such that said biometric template is not stored on said device in a form that is accessible without executing said TRS encoded access software application

and

(e) employing the biometric template which has been integrated into the access software application to evaluate biometric data provided by a user seeking to access the other application, system or software entity to provide an evaluation result which either permits or denies access by the user.

2. (canceled)
3. (canceled)
4. (canceled)
5. (canceled)
6. (canceled)
7. (canceled)
8. (canceled)
9. (canceled)
10. (canceled)
11. (canceled)
12. (canceled)
13. (canceled)
14. (canceled)
15. (canceled)
16. (canceled)
17. (canceled)
18. (canceled)
19. (canceled)
20. (canceled)
21. (canceled)
22. (canceled)
23. (canceled)
24. (canceled)
25. (canceled)
26. (canceled)
27. (canceled)
28. (canceled)
29. (canceled)
30. (canceled)

31. (previously presented) A method according to claim 1 whereby the evaluation result comprises a cryptographic key generated to be either correct to permit access by the user or

incorrect to deny access by the user, the cryptographic key being generated to be correct only when the user-provided biometric data is found to match the biometric template.

32. (previously presented) A method according to claim 1 whereby the evaluation result comprises branching to a distinct location of the access software application if the user-provided biometric data is found to match the biometric template.

33. (previously presented) A method according to claim 31 whereby the evaluation result comprises a key for a symmetric cipher having high entropy for its key length, if the user-provided biometric data is found to match the biometric template.

34. (previously presented) A method according to claim 31 whereby the evaluation result comprises private key of a public/private key pair, if the user-provided biometric data is found to match the biometric template.

35. (cancelled).

36. (previously presented) A method according to claim 31 whereby the incorrect cryptographic key is identical in bit-length to the correct cryptographic key.

37. (currently amended) A method according to claim 1 whereby the TRS encoding comprises mass data encoding for ~~date~~ data in array, table or message buffer form.